REMARKS

Claims 21-24, 27-29 and 32-34 remain in this application.

Summary of the Examiner's final rejection:

Claims 21-24, 27-29 and 32-34 were rejected as unpatentable over newly-cited USP 6,230,268 to Miwa et al in view of newly-cited USP 6,289,102 to Ueda et al.

The patent to Ueda et al is cited as teaching scrambling digital data with digital watermark, and then recording the scrambled digital data with digital watermark onto a medium.

Summary of USP 6,230,268 to Miwa et al:

This Miwa et al patent describes a secure data control system that uses an electronic watermark technique.

A control flag (CF) is prepared using the electronic watermark technique. This CF contains information as to how to control the data (see 700 of FIG.7).

A token is prepared. This token contains information as to how to control the data by using the content of the data (see 720 of FIG. 7).

The data and its embedded token are then distributed (see the output of FIG. 7).

FIG. 8 receives the distributed data and the CF is detected from the distributed data (see 800 of FIG. 8), the token is read when the CF is detected (see 820 and 840 of FIG. 8), and the data is controlled according to a control-rule of the token or the CF.

Subsequent data control is suppressed by modifying the token (see 840 of FIG. 8).

At col. 1, line 66, to col. 2, line 22, it is stated that the term electronic watermark technique means embedding information in media such as still images, voice and motion pictures, wherein the embedded information is generated by manipulating the data of the media.

FIG. 7 is a flowchart that shows how in step 700 a CF is imbedded in original data (i.e. image, voice, still image and motion picture data) using an electronic watermark technique.

In step 710 a portion of the data that contains the embedded CF is extracted, a token is prepared from this extracted data in step 720 using a one-way function, and in step 730 the token is appended to the data that has the CF embedded therein.

FIG. 8 receives the data from FIG. 7, which data may contain both a CF and a token. In step 800 it is determined if the data actually contains an embedded CF. If "NO", data control not restricted, and copying, recording and playback of the data can occur. If "YES", step 820 determines if the data also contains a token. If "NO", data control is inhibited, i.e. copying, recording or playback of the data is inhibited, and the FIG. 8 process ends. If "YES", data control is done in accordance with a predefined rule of the token (or the CF). (see col. 4, lines 10-23)

FIG. 5 shows the control-owner-side and the user-side of a copying control system that uses a one-way hash function. The FIG. 5 system prohibits more than one copy of data that is distributed from the content-owner-side to the user-side. This is accomplished by appending a token to digital data that is distributed to the user-side, using an electronic watermark technique, wherein the token is disabled once the data has been copied one time.

In FIG. 5 the content-owner-side calculates a token from the image data using a one-way hash function, and the token is distributed to the user-side along with the image data. (see col. 6, lines 51-55)

At the content-owner-side of FIG. 5 a token is appended to the data only when a CF which is embedded in the data by an electronic watermark technique indicates that the data may be copied once (see col. 7, lines 34-38), and at the user-side the token is authenticated as valid only when the CF that is embedded by the electronic watermark technique indicates that the distributed data can be copied one time (see col. 7, lines 49-51).

NOTE: In the final rejection the Examiner states "Miwa et al fail to teach an inventive concept of scrambling the digital data with digital watermark, and recording the scrambled digital data with digital watermark onto a medium".

Summary of USP 6,289,102 by Ueda et al:

This patent to Ueda et al provides a recording medium having a lead-in-area that contains key-information and a data recording-area in which scrambled data is recorded. The scrambled data is descrambled based on the key information.

A number of embodiments of the invention are described in the patent's DISCLOSURE OF THE INVENTION section, including the use of first and second key-information fields.

For example, in FIG. 1 scramble-information (see FIG. 2) within the lead-in area is read, this scramble-information is interpreted, and descramble-processing (see FIG. 9) is performed in accordance with this the scramble-information that was read.

Claim 1 defines an arrangement wherein this scramble-information (key-information) is accessible only by a disk-reproducing device.

Claim 2 defines an arrangement wherein first key-information is recorded in the lead-in-area, wherein a number of second key-information and the scrambled data, are recorded in the

data-recording-area, and wherein the descrambling of certain data is based upon a certain second key and the first key.

NOTE: In the final rejection the Examiner states "Ueda et al teach an inventive concept of scrambling the digital data with digital watermark, and recording the scrambled digital data with digital watermark onto a medium".

Discussion of the present invention:

The present invention operates to control copy or playback of digital data wherein a digital watermark is embedded within the digital data by way of a transformation of the digital data.

The present invention makes it possible to distribute original digital data in a safer manner than was possible in the prior art because the original digital data is scrambled/encrypted, and the scrambled digital data is then descrambled or decrypted (as stated at page 4, lines 20-25 of the present specification).

As stated at page 8, lines 5-12, of the present specification, while scrambling is a means for enciphering, scrambling is improved by the present invention's use of scrambling based upon an encryption key. The present invention's use of scrambling by an encryption key provides that there is no way to decode the scrambled digital data in the absence of the encryption key. Thus, it is possible to distribute the digital data in a safer manner than in the prior art.

When the present invention's FIG. 7 playback-control is explained (starting at page 8, line 14, of the present specification) it is pointed that at step 720 the scrambled digital data received at step 710 is "descrambled (decoded)". In addition, at step 760 it is determined

whether or not another encryption technique has been used, whereupon if the result of step 760 is "YES" the corresponding decoding process is performed.

Advantages of the present invention's scrambling with an encryption key is also discussed at page 13 of the present specification, beginning at line 26, whereat it is stated that copying of scrambled digital date is protected by scrambling with an encryption key, thus making it possible to disable playback, even though copying is done.

Scrambling is dictionary-defined as "disarranging the elements of a transmission in order to make the transmission unintelligible to interception".

Encoding is dictionary-defined as "converting information from one system of communication into another, especially to convert a message into a code for transmission."

Thus, it is respectfully submitted that the present specification's description of scrambling digital data by an encryption key clearly teaches that (1) elements of the digital data are disarranged, and (2) the digital data is converted into a code, such that (3) the scrambled/coded digital data can be descrambled/decoded only when the encryption key is used.

Further it is respectfully submitted (1) that the terms coded and encrypted are interchangeable, and (2) that the terms decoded and decrypted are interchangeable.

In order to more clearly distinguish the claims remaining in this application from the Examiner's citations, all have been amended to include this new, unusual and unobvious feature.

For example, independent claim 21 (Currently amended) requires scrambling/encoding the digital data and the digital watermark using an encryption key such that subsequent copying or playback of the scrambled/encoded digital data is inhibited in the absence of knowledge of said encryption key.

Independent claim 24 (currently amended) requires that digital data is scrambled/encoded using an encryption key, and that descrambling/decoding of read digital data requires using said encryption key.

Independent claim 27 (currently amended) requires that digital data be scrambled/encoded using an encryption key, and that descrambling/decoding of the scrambled/encoded digital data be performed using the encryption key, to thereby reproduce the original digital data.

Independent claim 32 (currently amended) requires that scrambling/encoding of data be performed using an encryption key, and that descrambling/decoding be performed using the encryption key, to thereby recover the original digital data.

In addition, all claims remaining in this application are limited to inhibiting copying or playback of the original data.

It is respectfully submitted that the whole of the claims remaining in this application, which includes the above-noted limitations, is not anticipated or render obvious by the Examiner's citations.

Cited USP 6,230,268 to Miwa et al discloses an action such as copy or playback by comparing an abstracted-token and an embedded-token that is detected from the digital-content, wherein the abstracted-token is generated by abstracting a compressed image. Generating a token from the abstract is kept secret, while generating an abstract from the token is open to the public using an asymmetric key. (see for example col. 8, lines 6-29).

Cited USP 6,289,102 to Ueda et al teaches the descrambling of scrambled data using a key, wherein the key is recorded in a lead-in area. This key is not subjected to a scrambling procedure along with the digital data (see for example col. 32, lines 24-44), and the key

information is subjected to an encryption separately from the scrambled sectors (see for example col. 19, lines 33-50).

Even when the teachings of cited USP 6,230,268 to Miwa et al are combined with the teachings of cited USP 6,289,102 to Ueda et al, the resulting combination provides only using a secret asymmetric key apart from the source scrambled digital data and the digital watermark. The combination does not teach scrambling such a key with the source digital data.

Reconsideration and allowance of the present application is respectfully requested.

Respectfully submitted,

HOLLAND & HART LLP

By: _____

Francis A. Sirr, Esq.
Registration No. 17,265
P.O. Box 8749
Denver, Colorado 80201-8749
(303) 473-2700, x2709

Date: 8/21/03

3122541_1.DOC